

**Method and apparatus for handling user's
attributes sharing between service providers**

FIELD OF THE INVENTION

5 **[0001]** The present invention generally relates to user's attributes sharing among a plurality of service providers. More particularly, the invention is pertaining to methods and apparatus for handling of a user's attributes sharing between an attribute provider and an attribute requestor through discovery service mechanisms.

10 **BACKGROUND**

15 **[0002]** The Internet is a growing network wherein services are provided by different organisations generally known as service providers. The most widely spread services in the Internet community are those generally referred to as web services whereby users can communicate with each other on personal basis, make business, carry out proceedings with governmental organizations, and many other active or passive activities that a user might carry out.

20 **[0003]** An important key to the success of these web services is the user's Identity and, more precisely, the security, authenticity, and privacy of a user accessing and operating a web service. In a quite simple and exemplary scenario involving e-commerce, a user might want to apply quite traditional shopping habits while merely using his personal computer at home to make use of different and available web services for shopping. Thus, the user would ask different suppliers in order to get different budgets for a product, the user would assess different business conditions to make a choice, and would eventually give
30 personal details and a valid charging reference for buying

the product. A valid charging reference might be in this context a credit card identity or a valuable assertion issued by a trustable organization such as a bank accepting the charging. With this exemplary scenario the above issues of user's security, authenticity and privacy, as well as some others to be further commented, may be reasonably introduced. On the one hand, the supplier user and likely the trustable organization want to ensure that the buying user is the one who claims, the buying user wants to have the highest level of security in order to prevent a fraudulent use of his credit card or bank reference accepting any charge, and both the supplier and the buying users want to keep their privacy to avoid other supplier and buying users to know the business conditions they might have mutually agreed on, for example.

[0004] The authentication of a user has been traditionally solved by the user providing an identity and a password to be authenticated by a service provider where the user has an account. Generally speaking, a user might likely have a different identity and password per service provider where the user accesses or where the user has accounts. The procedure to follow when several authentications have to be carried out for a user is unpleasant, tedious and likely unnecessary in some scenarios, especially from the user perspective. A first attempt to solve this drawback, thus making more attractive and dynamic the use of web services through service providers, is the introduction of the so-called Single Sign-On (SSO) services for a user. The current SSO principle states that users are authenticated just once with an Identity Provider (IdP) and are given access to all their subscribed services accessible through a number of service providers (SP) that accept such level of authentication or, in other words, a number of service providers (SP) that along with the Identity Provider (IdP) form a circle of trust. For the purpose of the present

invention, a circle of trust is a sort of agreement signed by a plurality of service providers and at least one Identity Provider whereby the formers firstly accept credentials from a user as a proof of having had a single sign-on authentication with the latter, and secondly offer a requested service to the user.

[0005] With this first attempt, a single sign-on (SSO) authentication of a user can be carried out within a circle of trust where a plurality of service providers (SP) and identity providers (IdP) are included, and wherein each service provider may provide web services to the user, on its own, or in co-operation with other service providers. As accessing a web service the user may be asked to provide a certain number of user's attributes, such as personal details, that the service providers might need for better customizing the service, or for further keeping a user's profile, or for other reasons.

[0006] On the other hand, an extreme privacy and security might preclude the user from getting closer to, and from achieving, other business opportunities. In the above example of e-commerce, a user might want to broadcast a certain shopping profile to a number of service providers where interesting products for the client are available in order to obtain different shopping conditions. In this scenario, when discussing said first attempt of supporting single sign-on authentication within a circle of trust, there might be user's attributes continuously asked to the user from several service providers, and this might be also unpleasant, tedious and likely unnecessary from the user perspective. A second attempt to improve the use of web services might be the sharing of user's attributes between services providers in a circle of trust and inasmuch as security and privacy are not seriously compromised.

[0007] At this stage some considerations have to be made in respect of currently existing art as well as standards in this field, and more specifically, in terms of what different fora accept to compromise on privacy and security and how to balance them with the development of emerging and sophisticated web services.

[0008] Liberty Alliance Project (hereinafter LAP) aims to develop a set of open technical specifications for web services. A first achievement of LAP was the Identity Federation Framework (Id-FF) enabling single sign-on using a federated network identity. The Id-FF according to LAP provides specifications for associating, connecting, and binding multiple accounts for a given Principal at various Liberty Alliance sites within a Circle of Trust. This Circle of Trust being regarded as the basis for building up a more material relationship of members in a Federation.

[0009] That is, the first attempt described above of supporting single sign-on in a circle of trust is a simplified view of the Liberty achievement, wherein a service provider (SP) may be regarded as a Liberty Alliance site; a user with the user's Identity may be regarded as a Principal having a federated network identity that can be authenticated by the Identity Provider (IdP), the Principal being likely regarded as a unique user or as a group of individuals.

[0010] LAP has also go further with the above second attempt to improve the use of web services by proposing, apart from the Id-FF, a so-called Identity Web Services Framework (Id-WSF) specifying the basis for privacy and security protection and, more specifically, LAP promotes and defines the Id-WSF for a permission-based attributes sharing. In this respect, LAP distinguishes two classes of policies for carrying out said permission-based attributes

sharing: policies established by the LAP processing components, namely component entities within the circle of trust, and policies established by individual Principals, namely the users. In short, LAP supports the above second
5 attempt of sharing user's attributes within the circle of trust inasmuch as the user so permits.

[0011] Prior to discussing other existing techniques or trends to improve the use of web services by sharing users' attributes, the concept and scope of such users' attributes
10 for LAP has to be clarified. On the one hand, an Attribute is understood under LAP as a distinct characteristic of a Principal, thus Principal's characteristics are said to describe the Principal. This definition of attribute made by Liberty harmonizes with the aim of a user's attribute as
15 recited throughout this document, as well as with general interpretations made by the public, such as an attribute being a quality regarded as a natural or typical part of somebody or something, and also an attribute being an object recognized as a symbol of a person or his position.

20 [0012] On the other hand, LAP goes beyond the attribute scope and introduces the concept of 'Resource' as either data related to some identity, or service acting on behalf of some identity; the former being a user's attribute in its most classical meaning, such as the user's postal
25 address for example; the latter being a sort of abstraction derived from currently emerging services and facilities that may also characterize a user in interaction with other users, such as a user's calendar where user's appointments may interact with corresponding other-user's appointments.
30 In particular, a user's calendar might be regarded as an exemplary user's attribute interesting to share with other users, for example, simply for appointment purposes, or for more sophisticated services such as the user booking at any time for dinner in a restaurant, and the restaurant making

an appointment in the user's calendar as a confirmation of the booking later on.

[0013] LAP has introduced the concept of Resource to include both, the former and the latter, whereas the term
5 user's attribute is preferred and maintained throughout the present document for the sake of simplicity. The user's attributes in the present document assume the distinction made by LAP and thus include a sort of identity-related attributes and a sort of service-related attributes for a
10 particular user. Nevertheless, and whenever necessary, both natures may be explicitly distinguished to focus on any particular aspects they might have.

[0014] Another interesting scenario appears where big players in the telecommunication market have several types
15 of access and core network technologies distributed along the countries where they operate for providing the users with access to telecom networks and to Internet. In this scenario, the OSA/PARLAY standardization group is working on the development of an open standard interface between
20 the core network and the service network. Therefore, a conventional architecture based on OSA/PARLAY comprises Applications that are formally included in a service network and deployed on Application Servers (AS), a number of Service Capability Features (SCF) representing interface
25 classes of the OSA/PARLAY interface and implemented in Service Capability Servers (SCS), an OSA/PARLAY Framework (OSA-FW) for providing framework capabilities to applications such as a controlled access to the Service Capability Features, and core network elements.

30 [0015] The Service Capability Features (SCF) in OSA/PARLAY may be regarded as a sort of service-related attributes for a particular user, accessed from different Application Servers that may be regarded as Service Providers, and the

Service Capability Features (SCF) thus being considered user's attributes that can be shared between service providers within the scope of the present invention.

5 **[0016]** OSA/PARLAY introduces a so-called Framework, which is aware of a Service level Agreement (SLA) signed between the network operator and the service providers, and this OSA/PARLAY Framework grants or denies access to service capability features on an SLA basis. That is, a given service provider is allowed to access a given number of
10 service capability servers with certain constraints, however, the permission to access a service capability feature for a user, namely the permission to share a user's attribute, is not tied to the user, but simply to the Service level Agreement (SLA) signed between the operator
15 and the service provider.

[0017] Currently existing techniques under LAP Id-WSF provides for a Discovery Service where each service provider, which hosts user's attributes, registers a sort of reference to the attributes, namely a so-called resource
20 offering, and from where other service providers fetch such resource offering for further accessing the attribute. Given the required level of privacy and security under LAP, the registration of a resource offering for a user's attribute in said Discovery Service can only be carried out
25 by a service provider upon explicit user's consent. In particular, LAP designates the service provider carrying out the registration of a resource offering as 'attribute provider' whereas any service provider fetching such resource offering is designated as 'attribute requestor'.

30 **[0018]** Apart from the explicit user's consent to share its user's attributes, the mechanism followed to register a user's attribute for sharing under LAP Id-WSF is not far from the one followed by OSA/PARLAY, but for the fact that

the registration of a resource offering in LAP is on a per user basis, whereas the registration of a service capability feature handled by a given service capability server is not done on per user basis but rather on per
5 service capability feature, that is, on a per attribute identifier basis.

[0019] In this respect, an object of the present invention is the provision of a mechanism whereby the sharing of user's attributes can be carried out independently of
10 requiring a user's consent that may be mandatory under certain scenarios and superfluous under others, whilst still compatible with the requirement of users' consents.

[0020] On the other hand, the use of a Discovery Service as explained above for LAP, as well as the OSA/PARLAY
15 Framework, may work in an acceptable manner for static user's attributes, or attributes that change very seldom. For instance, an exemplary static user's attribute may be a Service-related attribute where a service provider customizes its behaviour towards the user based on the
20 user's online calendar, which in particular might be available through another service provider. In case the service provider wants to send goods to the user, this service provider can query the user's online calendar to determine the best delivery date for the user, based on his
25 current appointments. This service is supposed to be always available at the same node or, at least, is supposed to change quite seldom. Still another exemplary static user's attributes might be an Identity-related attribute where a service provider may customize its appearance and behaviour
30 towards the user based on identity related attributes like a preferred language. In this way, the service provider may ask another service provider through the Discovery Service for the preferred language and may further communicate with

the user using this language. This service is likely always available at the same node as well.

[0021] However, none of the currently existing techniques work properly for dynamic attributes that change very often. These dynamic user's attributes might be data generated during a user's service session, which may even change during the session, or other data belonging to the master session for the user, this master session being open once the user has been authenticated and comprising access session data and service session data among others. For instance, an exemplary dynamic user's attribute may be a Service-related attribute where a service provider may customize its appearance and behavior towards a user based on user's roaming status or on access capabilities. In this way, the service provider may ask another service provider, which owns the attribute for the user's roaming status or access capabilities through the Discovery Service, and provide the user with different commercial offers depending on where the user is roaming, such as car rental information when the user is abroad. Also, the service provider contents can be customized for the user access capabilities only showing multimedia rich contents if the user is connected through a broadband connection. This kind of attributes may be available at different nodes, or at different network locations from a session to another, or may even change during a user session.

[0022] In principle, a user's attribute registered in a LAP Discovery Service or in an OSA/PARLAY Framework should be deregistered and registered again as the attribute changes, and always with user's consent under LAP, or other permission-based policies to apply under OSA/PARLAY. These continuous registrations of users' attributes imply in most of the cases the application of permission-based policies that might make no sense since there have been no new

condition to modify the previous policies applied. In fact, a user's attribute may be deregistered and registered again only due to a temporary limitation on broadband connection, for example, and this should not be appreciated as a
5 substantial change deserving application of permission-based policies again.

[0023] Thereby, an object of the present invention is the provision of a mechanism for sharing user's attributes whereby there is no need for carrying out continuous
10 procedures for deregistering and registering a user's attribute that changes very often.

[0024] Moreover, the fact that a service provider hosting a user's attribute, namely an attribute provider (AP), registers such user's attribute in a sort of Discovery
15 Service does not necessarily imply that said user's attribute is going to be shared from another service provider, namely from an attribute requestor (AR). Under this assumption, and especially for users' attributes changing very often, deregistering and registering such
20 users' attributes create an extremely high registration traffic towards the Discovery Service and quite unnecessary processing load without any actual sharing of the user's attribute.

[0025] Thereby, another object of the present invention is
25 an enhancement of the existing mechanisms for sharing of users' attributes so that the registration traffic towards a Discovery Service, or the like, is optimized for an actual sharing of such user's attribute.

SUMMARY OF THE INVENTION

30 **[0026]** The objects above, among other things, are accomplished in accordance with the invention by the

provision of means and methods for handling user's attributes sharing between Service Providers.

[0027] Thus, there is provided a method of handling user's attributes sharing between a plurality of Service Providers, a Service Provider being regarded as an Attribute Provider hosting at least one user's attribute for a user and offering such attribute for sharing with other Service Providers regarded as Attribute Requestors, an attribute offering being published in a Discovery Service Framework suitable for holding attribute offerings from at least one Attribute Provider and for providing any of such attribute offerings to at least one Attribute Requestor, the method originally comprising the steps of:

(a) the Attribute Provider registering an attribute offering in the Discovery Service Framework;

(b) the Attribute Provider providing the attribute upon request from an Attribute Requestor;

and wherein, in accordance with an aspect of the present invention, the above step a) is preceded in this method by previous steps of:

(c) the Attribute Provider registering an offering registration trigger in the Discovery Service Framework intended to request, if needed, the registration of the attribute offering; and

(d) the Attribute Provider receiving from the Discovery Service Framework a request for registration of the attribute offering.

[0028] Given that an offering registration trigger includes a minimum set of indications to request the registration of an attribute offering, an alternative embodiment of this method is proposed wherein the offering

registration trigger may be the same for all those users for which the Attribute Provider hosts users' attributes, whereas in another embodiment the offering registration trigger may be different for each user having a user's attribute hosted in an Attribute Provider.

[0029] Moreover, the step in this method of registering the offering registration trigger in the Discovery Service Framework may preferably include a step of registering policies intended to govern the lifetime of the offering registration trigger and, in a similar manner, the step of registering an attribute offering in the Discovery Service Framework may also include a step of registering policies intended to govern the lifetime of the attribute offering.

[0030] Depending on particular requirements on user's privacy and security in an applicable scenario, this method may comprise a step of obtaining a user's consent to share user's attributes.

[0031] Furthermore, in accordance with an embodiment of the invention, the offering registration trigger is preferably withdrawn once the user signs off whereas, in accordance with another alternative embodiment, just the attribute offering, and not the offering registration trigger, is withdrawn once the user signs off.

[0032] For the sake of completeness, there is provided a method of publishing through a Discovery Service Framework an attribute offering for sharing a user's attribute between a plurality of Service Providers, a Service Provider being regarded as an Attribute Provider hosting at least the user's attribute for which the attribute offering may be published, this Discovery Service Framework suitable for holding attribute offerings from at least one Attribute Provider, the method originally comprising the steps of:

(a) registering in the Discovery Service Framework an attribute offering upon request from an Attribute Provider;

5 (b) the Discovery Service Framework providing the attribute offering upon request from a Service Provider acting as an Attribute Requestor for the attribute offering;

and wherein, in accordance with a second aspect of the present invention, the above step a) is preceded in this method by previous steps of:

10 (c) registering an offering registration trigger in the Discovery Service Framework upon request from the Attribute Provider;

(d) the Discovery Service Framework processing the offering registration trigger upon request for an attribute offering received from an Attribute Requestor; and
15

(e) requesting the registration of the attribute offering to the Attribute Provider as a result of processing the offering registration trigger.

[0033] Also in this method, and in coordination with a
20 corresponding step in the previous method of handling user's attributes sharing, the step of registering the offering registration trigger in the Discovery Service Framework may preferably include a step of registering policies intended to govern the lifetime of the offering
25 registration trigger and, in a similar manner, the step of registering an attribute offering in the Discovery Service Framework may also include a step of registering policies intended to govern the lifetime of the attribute offering.

[0034] In particular, and in accordance with an embodiment
30 of the invention, the offering registration trigger may be withdrawn upon processing corresponding policies governing

its lifetime whereas, in accordance with another embodiment of the invention, just the attribute offering, and not the offering registration trigger, is withdrawn upon processing corresponding policies governing its lifetime.

5 **[0035]** Still further, in accordance with an embodiment of the invention, the offering registration trigger is preferably withdrawn upon request from the Attribute Provider where the user signs off whereas, in accordance with another alternative embodiment, just the attribute
10 offering, and not the offering registration trigger, is withdrawn upon request from the Attribute Provider where the user signs off.

[0036] Apart from the above methods, and in accordance with a third aspect of the invention, there is provided a
15 Discovery Service Framework suitable for holding an attribute offering registered from an Attribute Provider and for providing the attribute offering to an Attribute Requestor, the Attribute Provider and the Attribute Requestor being Service Providers enabled for sharing a
20 user's attribute, the Attribute Provider hosting at least the user's attribute to be shared, the Discovery Service Framework generally comprising:

- (a) a first input unit for processing an attribute offering received from an Attribute Provider;
- 25 (b) a storage for storing contents obtainable from the attribute offering;
- (c) a second input unit for processing a request received from an Attribute Requestor for an attribute offering; and
- 30 (d) a first output unit for providing the attribute offering to the Attribute Requestor;

and, in accordance with this third aspect, also comprising:

- (e) a third input unit for processing an offering registration trigger received from the Attribute Provider;
- 5 (f) a trigger handler for storing contents obtainable from the offering registration trigger and for determining trigger conditions to request a registration of the attribute offering; and
- (g) a second output unit for requesting the registration of
10 the attribute offering to the Attribute Provider.

[0037] This trigger handler is a component that may be used for determining the trigger conditions for requesting the registration of the attribute offering upon reception in the second input unit of a request for the attribute
15 offering from the Attribute Requestor. Nevertheless, the second input unit might be adapted to this end as well.

[0038] The trigger handler might also be usable for processing policies received in the third input unit, policies that are intended to govern the lifetime of the
20 offering registration trigger, though the third input unit itself might also be arranged for processing these policies as well. In this respect, other alternative embodiments, such as receiving policies in the first input unit, might be also advantageously carried out in order to reduce the
25 number of internal components.

[0039] Provided that the trigger handler component is present, it may further withdraw an offering registration trigger either upon processing corresponding policies governing its lifetime, or upon request received in a
30 fourth input unit from the Attribute Provider where the user signs off. Moreover, the trigger handler may also withdraw an attribute offering either upon processing

corresponding policies governing its lifetime, or upon request received in a fifth input unit from the Attribute Provider where the user signs off.

[0040] The Discovery Service Framework is complemented for achieving the objects of the present invention with an Attribute Provider arranged to this end. This Attribute Provider hosting a user's attribute for a user and offering such attribute for sharing with other Service Providers regarded as Attribute Requestors, an attribute offering for the user's attribute being published in a Discovery Service Framework suitable for holding attribute offerings from Attribute Providers and for providing any of such attribute offerings to Attribute Requestors. The Attribute Provider generally comprising:

- 15 (a) a first output unit for accessing the Discovery Service Framework to register an attribute offering;
- (b) a first input unit for processing a request received from an Attribute Requestor for the attribute offering; and
- 20 (c) a second output unit for providing the attribute offering to the Attribute Requestor;

and, in accordance with a fourth aspect of the present invention, further including:

- 25 (d) a third output unit for accessing the Discovery Service Framework to register an offering registration trigger; and
- (e) a second input unit for processing a request received from the Discovery Service Framework for registration of the attribute offering.

[0041] Preferably in this Attribute Provider, the third output unit may be used for accessing the Discovery Service Framework to register policies intended to govern the lifetime of the offering registration trigger, whereas the first output unit may be used for accessing the Discovery Service Framework to register policies intended to govern the lifetime of the attribute offering. In this respect, other arrangements may be provided where a unique unit may deal with policies related to both offering registration trigger, and attribute offering; or where a combination of a number of units deals with such policies.

[0042] As for a method commented above, and depending on particular requirements on the user's privacy and security, this Attribute Provider may further comprise:

- (f) a fourth output unit for requesting a user's consent to share a user's attribute; and
- (g) a third input unit for obtaining the user's consent to share a user's attribute.

[0043] For the sake of coherence with an above method, the third output unit may be used in an embodiment of the invention to register in the Discovery Service Framework a same offering registration trigger for all those users for which the Attribute Provider hosts users' attributes, or may be used in an alternative embodiment to register a different offering registration trigger for each user having a user's attribute hosted in the Attribute Provider.

[0044] The Attribute Provider may advantageously include a fifth output unit for accessing the Discovery Service Framework to withdraw an offering registration trigger upon the user signing off, and a sixth output unit for accessing the Discovery Service Framework to withdraw an attribute offering upon the user signing off. However, other

arrangements with re-use of other units, or combinations thereof, might be used as well.

[0045] In this respect, another advantageous embodiment may be the use of first and third output units, or a combination thereof, to register the offering registration trigger along with the actual attribute offering.

BRIEF DESCRIPTION OF DRAWINGS

[0046] The features, objects and advantages of the invention will become apparent by reading this description in conjunction with the accompanying drawings, in which:

[0047] FIG. 1 represents exemplary components in a prior art architecture for sharing user's attributes between an Attribute Provider and an Attribute Requestor with a Discovery Service Framework for publishing corresponding attribute offerings.

[0048] FIG. 2 shows a simplified sequence diagram representing the process followed in a prior art solution to share a user's attribute between an Attribute Provider and an Attribute Requestor by publishing a corresponding attribute offering in a Discovery Service Framework.

[0049] FIG. 3 represents an exemplary architecture with suitable components for sharing dynamic and static user's attributes between an Attribute Provider and an Attribute Requestor with a Discovery Service Framework for handling offering registration triggers corresponding to attribute offerings.

[0050] FIG. 4 shows a basic sequence diagram representing the process followed in accordance with the invention to share a user's attribute between an Attribute Provider and an Attribute Requestor by handling an offering registration

triggers corresponding to said user's attribute and by publishing a corresponding attribute offering in a Discovery Service Framework.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

5 [0051] The following describes currently preferred embodiments of means and methods for handling user's attributes sharing between service providers.

[0052] From a user's point of view, the procedure followed to register a user's attribute in a particular service
10 provider is not affected by the present invention. Thus, once the user (40) has been authenticated in the service provider (20), which for the purpose of the present invention plays the role of an Attribute Provider (AP), the service provider collects (S-112), as shown in Fig. 2, a
15 number of user's attributes, if not already done in a previous access from the user. At this stage, and provided that particular user privacy policies have to be taken into consideration, the user may indicate (S-106, S-107) a user's consent to share any particular user's attribute
20 hosted by that service provider (20).

[0053] In a solution as illustrated in Fig. 2, the service provider (20) hosting the user's attribute, namely the Attribute Provider, accesses a Discovery Service Framework (10), which is hereinafter referred to as DSF, for
25 registering an attribute offering (S-101) for such user's attribute to be offered. The DSF stores data extracted from this attribute offering in a local storage (F-db) and makes it public and accessible for other service providers (30) wanting to share such user's attribute. To this end, as
30 illustrated in Fig. 1, the Attribute Provider (20) is provided with its first output unit (POU-1) for accessing the DSF (10) to register the attribute offering (S-101),

and the DSF is provided with its first input unit (FIU-1) to receive registrations of attribute offerings (S-101).

[0054] At a later stage, the user (40) might have accessed another service provider (30) and, after having been
5 authenticated in this another service provider, the user may invoke a service that, for its complete execution, needs a user's attribute that is hosted in an external Attribute Provider (20). The another service provider (30) where the user has presently accessed, playing the role of
10 an Attribute Requestor, requests (S-102) the location of the user's attribute to the DSF (10). This request may be carried out by a 'DS Lookup Query' operation. Upon receipt of such request, the DSF fetches relevant information about an attribute offering for such user's attribute in its
15 local storage (F-db), and sends it back (S-103) to the Attribute Requestor (30). To this end, as illustrated in Fig. 1, the Attribute Requestor (30) is provided with its first output unit (ROU-1) for accessing the DSF (10) to query (S-102) about the user's attribute and its first
20 input unit (RIU-1) for receiving (S-103) the expected response, whereas the DSF (10) is provided with its second input unit (FIU-2) for receiving such query (S-102) and its first output unit (FOU-1) for sending the response (S-103).

[0055] Eventually, the Attribute Requestor (30) makes use
25 of the relevant location data obtained from the attribute offering held in the DSF for accessing (S-104) to the Attribute Provider (20) to request the user's attribute hosted in said Attribute Provider (20) and to be presently shared (S-105) with this Attribute Requestor (30). As shown
30 in Fig. 1, the Attribute Requestor is provided with its second output unit (ROU-2) for accessing the Attribute Provider (S-104) and with its second input unit (RIU-2) for receiving the requested user's attribute (S-105), whereas the Attribute Provider (20) includes a first input unit

(PIU-1) for receiving requests (S-104) to share a user's attribute from an Attribute Requestor (30) and a second output unit (POU-2) for sharing (S-105) a requested user's attribute.

5 **[0056]** In accordance with the invention this process and corresponding means are enhanced to accomplish the objects of the invention.

10 **[0057]** The process illustrated in Fig. 4 assumes that the user's attributes had been collected in a previous access and are already hosted in the Attribute Provider (20), and that the user (40) has given consent (S-106, S-107) for sharing user's attributes. Provided that such user's attributes had not been collected before, the collection can be carried out (S-112) in a similar manner as the one shown in Fig. 2. Therefore, as also shown in Fig. 3, the Attribute Provider may include a particular output unit (POU-4) for requesting (S-106) the user's attributes and likely the user's consent, and with a particular input unit (PIU-3) for getting (S-107) user's attributes and for being
15 granted or denied such user's consent.
20

25 **[0058]** The process in Fig. 4 follows with the Attribute Provider (20) accessing the DSF (10) for registering an offering registration trigger (S-108) intended to further request a registration of an actual attribute offering upon request, if any, from another service provider (30) playing the role of an Attribute Requestor (AR). The DSF stores data extracted from this offering registration trigger in a trigger handler (TH), and makes it public and accessible for other service providers (30) wanting to share a
30 corresponding user's attribute. To this end, as illustrated in Fig. 3, the Attribute Provider (20) is provided with a third output unit (POU-3) for accessing the DSF (10) to register the offering registration trigger (S-108), and the

DSF is provided with a third input unit (FIU-3) to receive registrations of offering registration triggers (S-108) and with a trigger handler (TH) for handling triggers and determining trigger conditions to request a registration of an actual attribute offering. In particular, an offering registration trigger may be the same for all those users for which the Attribute Provider (20) hosts users' attributes, or may be different for each user having a user's attribute hosted in the Attribute Provider.

10 **[0059]** Moreover, the registration of the offering registration trigger (S-108) may be accompanied by a registration of policies intended to govern the lifetime of said offering registration trigger (S-108). Therefore, the third output unit (POU-3) may be preferably used.

15 **[0060]** In Fig. 4 and as already explained when commenting the process illustrated in Fig. 2, the user (40) might have accessed (S-113) another service provider (30) at a later stage and, after having been authenticated in this another service provider, the user may invoke a service (S-114)
20 that needs a user's attribute hosted in an external Attribute Provider (20).

[0061] This another service provider (30) where the user has presently accessed, requests (S-102) as an Attribute Requestor (AR) the location of the user's attribute to the
25 DSF (10), having to this end the first output unit (ROU-1) of the Attribute Requestor for issuing the query (S-102) and the second input unit (FIU-2) of the DSF for receiving the request (S-102).

[0062] Upon receipt of such request, the DSF fetches
30 relevant information about an attribute offering for such user's attribute in its local storage (F-db), and does not find a proper attribute offering since, in this case, such attribute offering has not been registered yet from an

Attribute Provider (20). The DSF, however, determines a trigger condition from the query received in the second input unit (FIU-2) matching with significant information of an offering registration trigger handled in the trigger handler (TH). This trigger condition makes the DSF request (S-109) a registration of the attribute offering to the Attribute Provider (20) hosting a corresponding user's attribute. Therefore, the DSF is provided in accordance with the invention and shown in Fig. 3 with a second output unit (FOU-2) for requesting (S-109) the registration of the attribute offering to the Attribute Provider (20), this second output unit (FOU-2) locally connected to the trigger handler (TH), and the trigger handler co-operating with the second input unit (FIU-2) for determining the trigger condition, whereas the Attribute Provider (20) includes a second input unit (PIU-2) for receiving and processing such request (S-109).

[0063] The reception of this request (S-109) in the Attribute Provider (20) is followed by a step of accessing the DSF to register the attribute offering (S-101) for such user's attribute to be offered. Therefore, as illustrated in Fig. 3, the Attribute Provider (20) includes its first output unit (POU-1) for accessing the DSF (10) to register the attribute offering (S-101), and the DSF is provided with its first input unit (FIU-1) to receive registrations of attribute offerings (S-101).

[0064] Furthermore, the registration of the attribute offering (S-101) may be accompanied by a registration of policies intended to govern the lifetime of said attribute offering (S-101). Therefore, the first output unit (POU-1) may be preferably used as well.

[0065] As receiving the requested registration of the attribute offering (S-101), the DSF stores data extracted

from this attribute offering in the local storage (F-db), likely with accompanying policies, and makes it public and accessible for other service providers (30) wanting to share such user's attribute. Given that this registration
5 had been triggered upon conditions derived from a request (S-102) received from an Attribute Requestor (30), the DSF fetches relevant information about the attribute offering and sends it back (S-103) to the Attribute Requestor (30). To this end, as Fig. 1 and Fig. 3 illustrate, the Attribute
10 Requestor (30) is provided with its first output unit (ROU-1) for accessing the DSF (10) to query about the user's attribute and its first input unit (RIU-1) for receiving the expected response, whereas the DSF (10) is provided with its second input unit (FIU-2) for receiving such query
15 (S-102) in connection with the trigger handler (TH) and the local storage (F-db), and it is also provided with its first output unit (FOU-1) for sending the response (S-103).

[0066] At this point, it is worthwhile to notice that the DSF may likely belong to the Identity Provider domain where
20 the user belongs to, though the invention is not constrained to such particular scenario.

[0067] In an alternative embodiment, which is especially relevant for those attribute offerings corresponding to user's attributes that do not change very often, both
25 offering registration trigger and actual attribute offering may be simultaneously registered, and likely including corresponding policies governing its respective lifetime. Therefore, different arrangements may be provided such as having a unique combination of first and third output units
30 (POU-1, POU,3) at the Attribute Provider (20), and a unique corresponding combination of first and third input units (FIU-1, FIU-3) at the Discovery Service Framework (10). Indeed, separate units as in previous embodiments with a suitable co-ordination may be used as well to this end.

[0068] Eventually, withdrawal of offering registration triggers and actual attribute offerings may be respectively carried out at the DSF (10) either upon processing corresponding policies governing its respective lifetime, or upon request (S-110, S-111) from the Attribute Provider (20) once the user (40) signs off.

[0069] On the one hand, in accordance with an embodiment of the invention for withdrawal due to policies processing, the trigger handler (TH) at the DSF (10) may be used to withdraw an offering registration trigger as a result of processing corresponding policies, which are preferably handled at said trigger handler (TH), whereas the local storage (F-db) may be provided with processing capabilities to withdraw an attribute offering as a result of processing corresponding policies. In another alternative preferred embodiment, all policies applying to offering registration triggers and actual attribute offerings are handled by the trigger handler (TH) and, thereby, the withdrawal of any attribute offering might as well be carried out from the trigger handler (TH) by applying corresponding policies.

[0070] On the other hand, in accordance with an embodiment of the invention for withdrawal due to the user signing off, the trigger handler (TH) at the DSF (10) may also be used to withdraw an offering registration trigger as a result of receiving a request (S-110) from the Attribute Provider (20) once the user (40) has signed off. Therefore, the Attribute Provider (20) may include a fifth output unit (POU-5) for requesting withdrawal (S-110) of an offering registration trigger, and the DSF (10) may include a fourth input unit (FIU-4) for receiving such request (S-110) and for requesting the trigger handler (TH) to proceed accordingly. Moreover, the Attribute Provider (20) may also include a sixth output unit (POU-6) for requesting withdrawal (S-111) of an attribute offering, and the DSF

(10) may include a fifth input unit (FIU-5) for receiving such request (S-111). Upon receiving (S-111) a request for withdrawal at the fifth input unit (FIU-5), the latter may request the trigger handler (TH) such withdrawal as well as
5 corresponding policies for the attribute offering. However, the fifth input unit (FIU-5) might as well request the withdrawal to the local storage (F-db) where relevant data for the attribute offering are handled, and the latter, depending on whether policies for attribute offerings are
10 stored in said local storage or in the trigger handler, may carry out such withdrawal locally or requesting the trigger handler to act correspondingly.

[0071] The invention is described in respect of several embodiments in an illustrative and non-restrictive manner.
15 Modifications of the embodiments are possible in light of the above teachings, and those modifications that fall within the scope of the claims are intended to be included therein.